

Актуальные вопросы защиты информации в компьютерных сетях

Баранов А.П.
ГНИВЦ ФСН России,
НИУ ВШЭ

Можно ли защитить в «облаке» конфиденциальную информацию?



Корпоративное
«облако»

100.000 пользователей



Публичное
«облако»

Более миллиона пользователей

4 составляющие «облака», основанного на VM.

- 1. Телекоммуникационная составляющая, аппаратные компоненты ЦОДа, пользователи
- 2. «Средний» (Middleware) слой, обеспечивающий VM
- 3. Прикладные сервисы предоставляемые ЦОДом
- 4. Системы хранения данных

Можно ли обеспечить безопасность на сертифицируемом уровне?

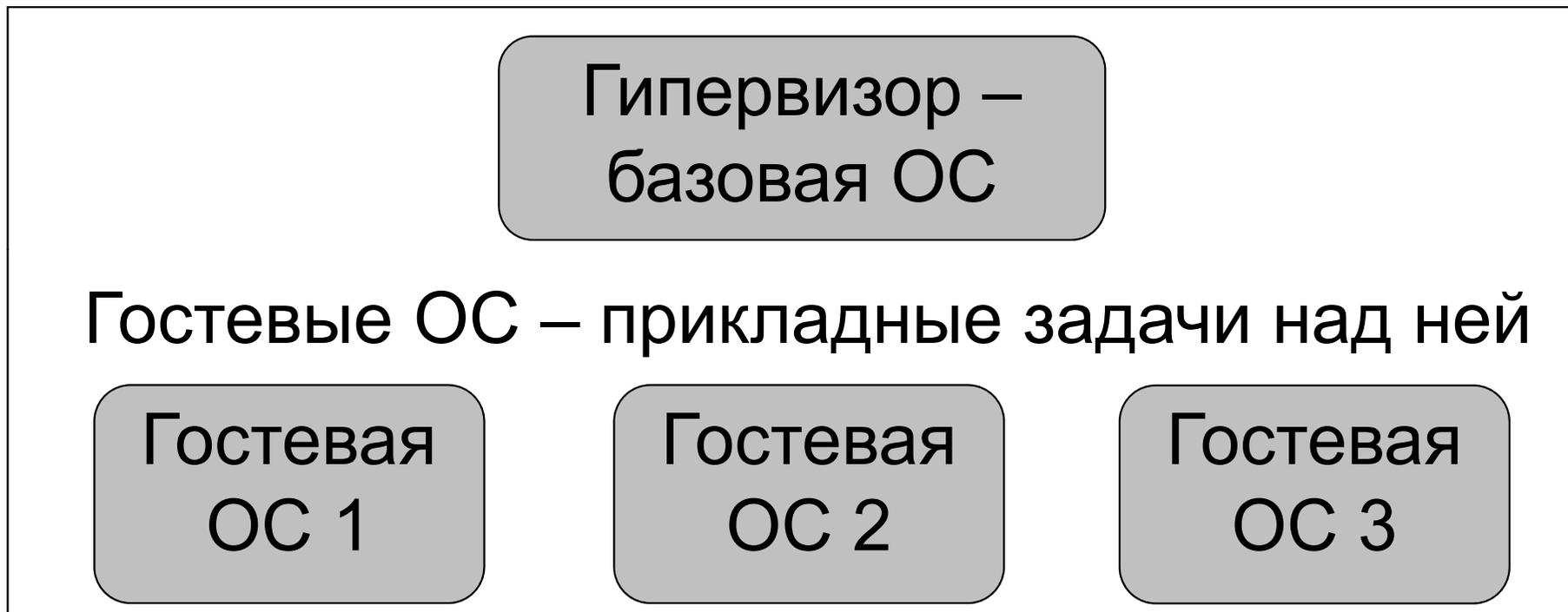
- **Телекоммуникация - IP криптография**
- Корпоративное «облако»: выделенная VPN-сеть 100.000 пользователей, древовидная структура связей, IP шифраторы до 1 Гбит/сек
- Контроль пользователей на уровне рабочих мест

Публичное «облако»

- Internet-сеть доступа, более миллиона пользователей, рабочие места (PM) смешанного типа
- Нет контроля пользовательских PM
- IP – шифрование: шифртехника в ЦОД до 100 Гбит/сек на PM более 1 Мбит/сек
- Протокол SSL. Требуется сертификация

Средний слой (Middleware)

Представление:



Сертификация как ОС – Microsoft, SUN, Linux, MC VC

- Исходные тексты?

Аттестация прикладных сервисов

- Прикладные сервисы аналогичны по аттестации прикладному ПО над обычными ОС.
- Главное – выработка требований по безопасности в ходе сертификации гипервизора.

Системы хранения данных

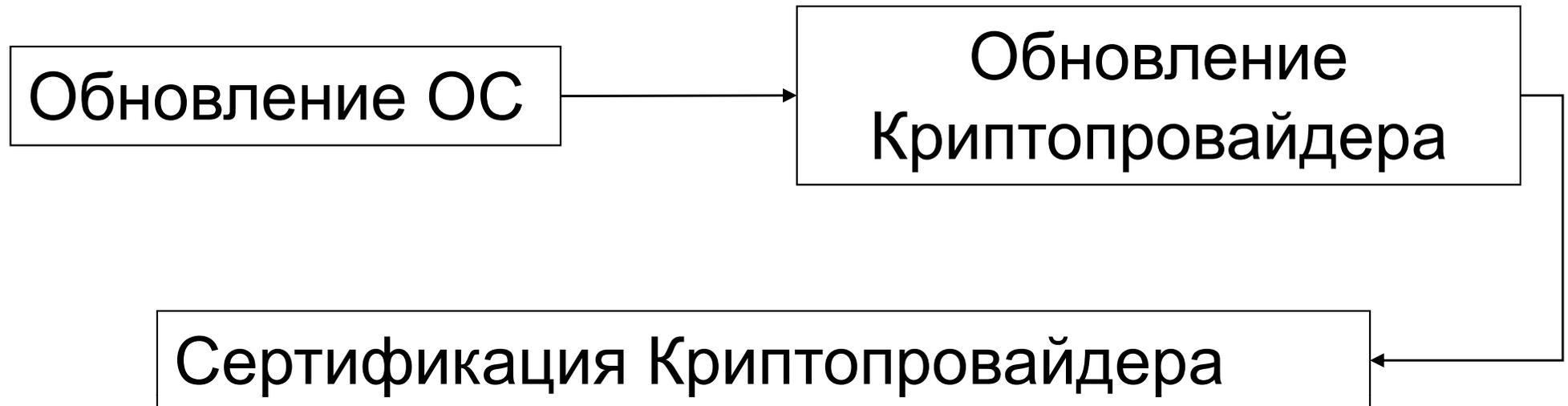
- В настоящее время сертифицирована только СУБД MS SQL
- Надо сертифицировать до категории 1-Г по требованиям ФСТЭК Oracle, IBM DB2 или что-то сопоставимое
- По аналогии с ОС компоненты «облачных» вычислений могут быть сертифицированы за 2-3 года со сравнимыми затратами

Актуальные проблемы криптографии

- 1. Проблема стандартизации шифрования в IP протоколе и обеспечение совместимости
- 2. Стандартизация и синхронизация ключевых структур
- 3. Стандартизация реализации SSL протокола. Стыковка различных производителей

Актуальные проблемы криптографии

- 4. Стандартизация реализаций ЭЦП.
Единое пространство доверия
- 5. Сокращение времени сертификаций
обновлений (2 раза в год):



Актуальные проблемы криптографии

- 6. Сертификация и стандартизация «простой» Электронной подписи.
Возможные аналоги: системы Свой-Чужой, Имитоприставки и др. парольные системы.

Нужна ли общественная сертификация или лицензирование в области защиты конфиденциальной информации не содержащий Гостайну?